IN THE CLAIMS:

1   1-15 (canceled)

1   16. (currently amended) A process for protecting a software product, sent from a server

2   computer to a computer, from unauthorized usage, the process comprising the steps of:

3   generating a first set of parameters from the computer before the software product

4   is ~~sent to the computer~~ encrypted at the server,

5   sending the first set of parameters to the server computer before the software

6   product is ~~sent to the computer~~ encrypted at the server,

7   creating, at the server computer, a single value from the first set of parameters be-

8   fore the software product is ~~sent to the computer~~encrypted at the server,

9   encrypting, at the server computer, the software product by using the single value

10   as the encryption key,

11   sending the encrypted software product to the computer,

12   encrypting, at the server computer, the single value by using members of the first

13   set of parameters as encryption keys, to form a set of encrypted single values,

14   sending the set of encrypted single values to the computer,

15   generating a second set of parameters from the computer,

16   decrypting members of the set of encrypted single values using members of the

17   second set of parameters as decryption keys, and

18   decrypting the encrypted software product by using the single value as the decryp-

19   tion key.

1   17. (currently amended) The process of claim 16 wherein the software product com-

2   prises ay least one data file ~~data files~~ or streaming data or both.

1   18. (currently amended) A process for protecting a software product, sent from a server

2   computer to a computer, from unauthorized usage, the process comprising the steps of:

3   generating a first set of parameters from the computer before the software product

4   is ~~sent to the computer~~ encrypted at the server,

5   sending the first set of parameters to the server computer before the software

6   product is encrypted at the server,

7   creating, at the server computer, a single value from the first set of parameters~~,~~

8   before the software product is encrypted at the server,

9   encrypting, at the server computer, the single value using members of the first set

10   of parameters as encryption keys, to form a set of encrypted values,,

11   sending the set of encrypted single values to the computer,

12   sending the software product to the computer,

13   generating a second set of parameters from the computer,

14   decrypting, at the computer, members of the set of encrypted single values by us-

15   ing members of the second set of parameters as decryption keys, and

16   authorizing access to the software product at the computer.

1   19. (currently amended) The process of claim 18 wherein the software product com-

2   prises ~~data files~~ at least one data file or streaming data or both.

1   20. (currently amended) The process of claim 18 further comprising the step wherein if

2   the said decryption yields a ~~number~~ quorum of identical single values, then

3   authorizing access to the software product at the computer.

1   21. (previously presented) A process for restricting a software product, downloaded

2   from a server computer to a computer, to only execute on the computer comprising, the

3   process comprising the steps of:

4   encrypting, at the server computer, the software product using a first encryption

5   key created from a first set of data collected from the computer,

6   encrypting, at the server computer, the first encryption key by using the first set of

7   data as the encryption key,

8   downloading the encrypted first encryption key to the computer,

9   downloading the encrypted software product to the computer,

10   requesting access to the encrypted software product at the computer, and in re-

11   sponse thereto, generating a second set of data from the computer,

12   decrypting the encrypted first encryption key using the second set of data as the

13   decryption key,

14   decrypting the encrypted software product by using the resultant of said decryp-

15   tion of the encrypted first encryption key as the decryption key.

1   22. (currently amended) The process of claim 21 wherein the software product com-

2   prises ~~data files~~at least one data file or streaming data or both.

1   23. (previously presented) A process for protecting a software product, sent from a

2   server computer to a computer, from unauthorized usage, the process comprising the

3   steps of:

4   encrypting, at the server computer, the software product before it has been sent to

5   the computer by using a first set of data collected from the computer as the encryption

6   key,

7   sending the encrypted software product to the computer, requesting access to the

8   encrypted software product at the computer, and in response thereto,

9   generating a second set of data from the computer, and

10   decrypting the encrypted software product by using the second set of data as the

11   decryption key.

1   24. (currently amended) The process of claim 23 wherein the software product com-

2   prises ~~data files~~at least one data file or streaming data or both.

1   25. (currently amended) A process for protecting a software product, sent from a server

2   computer to a computer, from unauthorized usage, the process comprising the steps of:

3   generating a first set of parameters from the computer before the software product

4   is ~~sent to the computer~~ encrypted at the server,

5   sending the first set of parameters to the server computer, before the software

6   product is encrypted at the server,

7   creating, at the server computer, a single value from the first set of parameters,

8   before the software product is encrypted at the server,

9   encrypting, at the server computer, the single value by using members of the first

10   set of parameters as the encryption keys, to form a set of encrypted values,

11   sending the set of encrypted single values to the computer,

12   sending the software product to the computer,

13   generating a second set of parameters from the computer,

14   decrypting members of the set of encrypted single values by using members of the

15   second set of parameters as the decryption keys, and

16   authorizing the execution of the software product on the computer.

1   26. (currently amended) The process of claims 25 further comprising the step wherein if

2   the said decryption yields a ~~number~~ quorum of identical single values, then

3   authorizing the execution of the software product on the computer.

1   27. (currently amended) The process of claim 25 wherein the software product com-

2   prises ~~data files~~at least one data file or streaming data or both.

1 28. (currently amended) A process for protecting a software product from unauthorized

2 usage by authenticating a computer before the software product is downloaded from a

3 server computer to the computer, the process comprising the steps of:

4 executing a license agreement by a user for the software product for the computer,

5 before the software product is downloaded to the computer,

6 and in response thereto, generating a first set of parameters from the computer be-

7 fore the software product is downloaded to the computer,

8 and sending the first set of parameters to the server computer before the software

9 product is downloaded to the computer,

10 storing the first set of parameters at the server computer,

11 instructing a software application, performed by a user, to download the software

12 product, and in response thereto, generating a second set of parameters from the com-

13 puter, and sending the second set of parameters to the server computer before the soft-

14 ware product is downloaded to the computer,

15 ~~omparing~~comparing, at the server computer, the first set of parameters to the sec-

16 ond set of parameters, and

17 ~~starting the download of~~downloading the software product to the computer.

1 29. (currently amended) The process of claim 28 wherein the software product com-

2 prises ~~data files~~at least one data file or streaming data or both.

1 30. (previously presented) The continuing process of claim 28 further comprising the

2 steps of: if the said download fails or is paused,

3 generating a third set of parameters from the computer,

4 sending the third set of parameters to the server computer,

5 comparing, at the server computer, the third set of parameters with the first or

6 second set of parameters stored at the server, and

7 resuming the download of the software product to the computer.

1 31. (currently amended) The process of protecting a software product from unauthorized

2 usage, sent from a sever computer to a computer, the process comprising the steps of:

3   generating a set of data from the computer before the software product is ~~sent to~~

4 ~~the computer~~encrypted at the server,

5   sending the set of data to the server computer before the software product is ~~sent~~

6 ~~to the computer~~encrypted at the server,

7   encrypting, at the server computer, the software product by using an encryption

8 key created from the set of data,

9   sending the encrypted software product to the computer,

10   generating a second set of data from the computer, and

11   decrypting the encrypted software product by using a decryption key created from

12 the second set of data.

1 32. (currently amended) The process of claim 31 wherein the software product com-

2 prises ~~data files~~at least one data file or streaming data or both.

33–36 (canceled)

1 37. (new) A system for protecting a software product, sent from a server computer to a

2 computer, from unauthorized usage, the system comprising:

3   means for encrypting the software product, at a server, before it has been sent to

4 the computer by using a first set of data collected from the computer as the encryption

5 key,

6   means for sending the encrypted software product to the computer,

7   means for requesting access to the encrypted software product at the computer,

8 and means for generating a second set of data from the computer and means for decrypt-

9 ing the encrypted software product by using the second set of data as a decryption key.

1   38. (new) A system for protecting a software product from unauthorized usage by au-

2   thenticating a user's computer before the software product is downloaded from a server

3   computer to the computer, the system comprising:

4   means for executing a license agreement for the software product for the com-

5   puter, before the software product is downloaded to the computer,

6   means for generating a first set of parameters from the computer

7   means for sending the first set of parameters to the server computer before the

8   software product is downloaded to the computer, means for storing the first set of pa-

9   rameters at the server computer,

10   means for instructing to download the software product,

11   means for generating a second set of parameters from the computer

12   means for sending the second set of parameters to the server computer before the

13   software product is downloaded to the computer,

14   means for comparing, at the server computer, the first set of parameters to the

15   second set of parameters, and

16   means for downloading the software product to the computer.

1   39. (new) A system for protecting a software product from unauthorized usage, sent from

2   a sever computer to a computer, the system comprising:

3   means for generating a set of data from the computer before the software product is en-

4   crypted at the server

5   means for sending the set of data to the server computer before the software prod-

6   uct is encrypted at the server,

7   means for encrypting, at the server computer, the software product by using an

8   encryption key created from the set of data,

9   means for sending the encrypted software product to the computer,

10   means for generating a second set of data from the computer, and

11   means for decrypting the encrypted software product by using a decryption key

12   created from the second set of data.

9